Basic Fundamentals Of Safety Instrumented Systems

- Overview
- Definitions of basic terms
- Basics of safety and layers of protection
- Basics of Safety Instrumented Systems
- Safety Integrity Level (SIL)
- Probability of failure upon Demand (PFD)
- Quiz

Overview

The operation of many industrial processes, especially those in the chemical or oil & gas industries, involve inherent risk due to the presence of dangerous chemicals or gases. Safety Instrumented Systems (SIS) are specifically designed to protect personnel, equipment, and the environment by reducing the likelihood or the impact severity of an identified emergency event.

Explosions and fires account for millions of dollars of losses in the chemical or oil & gas industries each year. Since a great potential for loss exists, it is common for industry to employ Safety Instrumented Systems (SIS) to provide safe isolation of flammable or potentially toxic material in the event of a fire or accidental release of fluids.

This course will explain the basic concepts, definitions and commonly used terms in Safety Instrumented Systems and provide a basic understanding of SIS related concepts.

Definitions

Following are common terms related to Safety Instrumented Systems.

Covert Fault: Faults that can be classified as hidden, concealed, or undetected.

Dangerous Failure: Failure which has the potential to put the safety instrumented system in a hazardous or fail−to−function state.

Demand: A condition or event that requires the safety instrumented system to take appropriate action to prevent a hazardous event from occurring, or to mitigate the consequence of a hazardous event.

Mitigation Layer: A protection layer that reduces the consequences of a hazardous event. Examples include emergency depressurization on detection of confirmed fire or gas leak.

Overt Faults: Faults that are classified as announced, detected, or revealed.

Prevention Layer: A protection layer that reduces the frequency of occurrence of a hazardous event.

Probability of Failure on Demand (PFD): A value that indicates the probability of a system failing to respond to a demand. The average probability of a system failing to respond to a demand in a specified time interval is referred as PFDavg. PFD equals 1 minus Safety Availability.

Process Hazard Analysis: It requires identifications of hazards, causes of accidents, possible outcome of accidents, safeguard to prevent and recommendation to implement measures to reduce process risk.

Protection Layer: Any independent mechanism that reduces risk by control, prevention or mitigation. This could be a process engineering mechanism such as the size of vessels containing hazardous chemicals etc., a mechanical engineering mechanism such as a relief valve, a safety instrumented system or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions.

Proven-In-Use: A component may be considered as proven-in-use when a documented assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system.

Redundancy: Use of multiple elements or systems to perform the same function. Redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

Reliability: Probability that a system can perform a defined function under stated conditions for a given period of time.

Safe Failure Fraction: Safe failure fraction (SFF) is a relatively new term resulting from the IEC 61508 and IEC 61511 committees' work to quantify fault tolerance and establish the minimum level of redundancy required in a safety instrumented function. Per IEC, "Safe failure fraction is the ratio of the (total safe failure rate of a subsystem plus the dangerous detected failure rate of the subsystem) to the total failure rate of the subsystem." (In IEC terms, subsystem refers to individual devices.)

There are four types of random hardware failures:

Safe undetected (^{SU});
Safe detected (^{SD});
Dangerous detected (^{DU});
Dangerous undetected (^{DD}).

Determining the SFF requires dividing the sum of the first three by the sum of all four. The assumption is that the operator is expected to take action based on the dangerous detected faults, therefore even if a device has a large fraction of dangerous failures, if enough can be detected and safe action taken, then the device is still considered a safe device.

The formula for determining the safe failure fraction (**SFF**) is:

$$\frac{\lambda^{SU} + \lambda^{SD} + \lambda^{DD}}{\lambda^{SU} + \lambda^{SD} + \lambda^{DU} + \lambda^{DD}}$$

Safe State: State that the equipment under control, or the process, shall attain as defined by the Process Hazard Analysis (PHA).

Safety Instrumented Function (SIF): Safety function with a specified safety integrity level, which is necessary to achieve functional safety. A safety instrumented function can be either a safety instrumented protection function (define SIPF) or a safety instrumented control function (define SICF).

Safety Instrumented System (SIS): Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensors, logic solvers, and final elements. This can include safety instrumented control functions, safety instrumented protection functions, or both.

Safety Integrity Level (SIL): SIL is a quantifiable measurement of risk used as a way to establish safety performance targets for SIS systems.

Spurious Trip: Refers to the shutdown of the process for reasons not associated with a problem in the process that the safety instrumented system is designed to protect (e.g., the trip resulted due to a hardware fault, software fault, electrical fault, transient, ground plane interference, etc.). Other terms used include nuisance trip and false shutdown.

Tolerable Risk: Risk which is accepted in a given context based on current values of society.

Basis of Safety and Layers of Protection

Safety is provided by layers of protection. These layers of protection start with safe and effective process control, extend to manual and automatic prevention layers, and continue with layers to mitigate the consequences of an event.

The first layer is the basic process control system. The process control system itself provides significant safety through proper design of process control.

The next layer of protection is also provided by the control system and the control system operators. Automated shutdown routines in the process control system combined with operator intervention to shut down the process are the next layer of safety.

Next is the SIS. It is a safety system independent of the process control system. It has separate sensors, valves, and logic system. Its only role is safety. No process control is performed in this system.

These layers are designed to prevent a safety related event. If a safety related event occurs there are additional layers designed to mitigate the impact of the event.

The next layer is an active protection layer. This layer may have valves or rupture disks designed to provide a relief point that prevents a rupture, large spill, or other uncontrolled release that can cause an explosion or fire.

The next layer is a passive protection layer. It may consist of a dike or other passive barrier that serves to contain a fire or channel the energy of an explosion in a direction that minimizes the spread of damage.

The final layer is plant and emergency response. If a large safety event occurs this layer responds in a way that minimizes ongoing damage, injury, or loss of life. It may include evacuation plans, fire fighting, etc.

Overall safety is determined by how these layers work together. The subject of this course is the safety instrumented system which is the final active prevention layer.

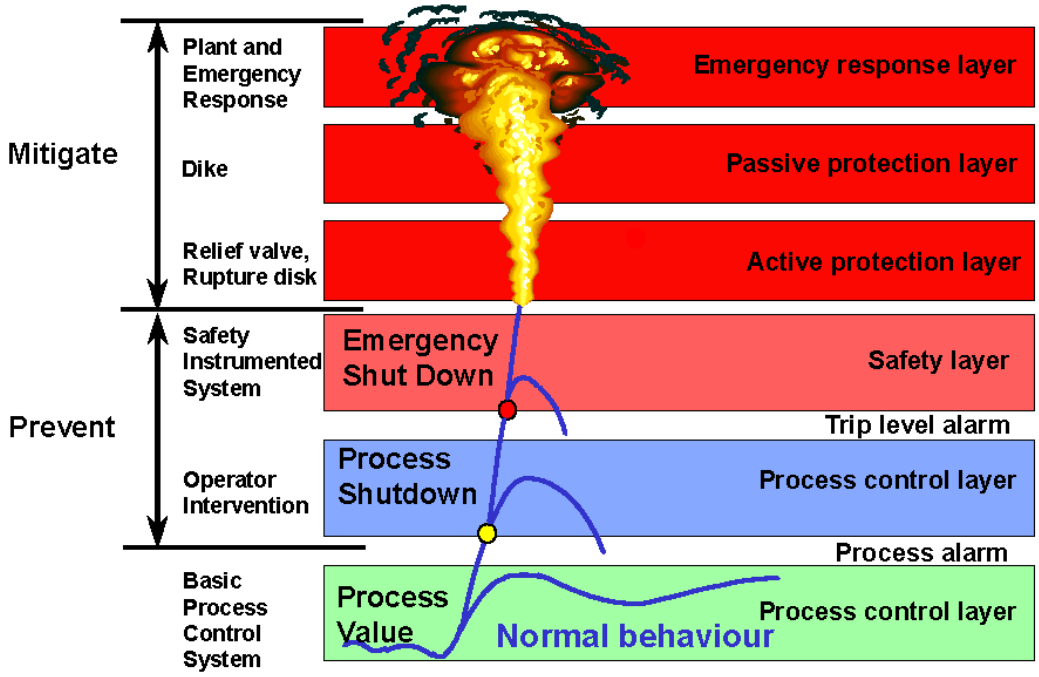


Figure 1. Depiction of Layers of Protection

Basics of Safety Instrumented System

Typically, safety instrumented systems consist of three elements as shown in figure 2.

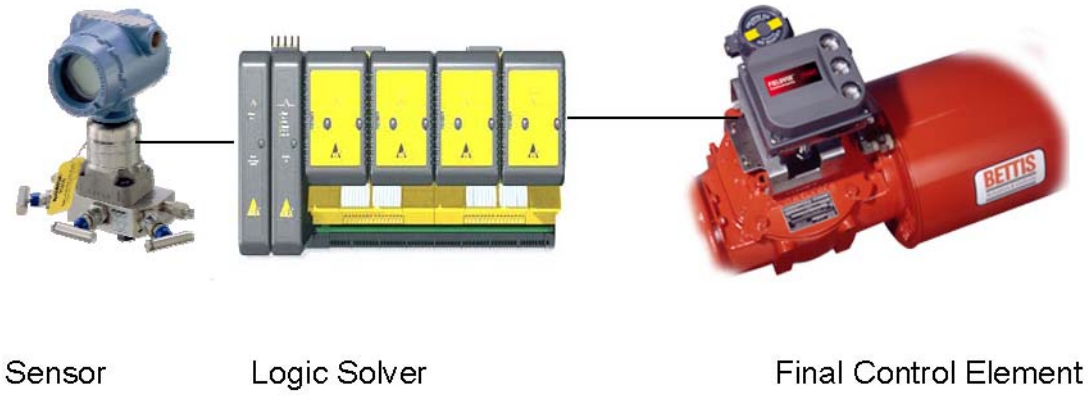


Figure 2. Components of Safety Instrumented System

Sensors: Field sensors are used to collect information necessary to determine if an emergency situation exists. The purpose of these sensors is to measure process parameters (i.e. Temperature, pressure, flow, density etc.) used to determine if the equipment or process is in a safe state. Sensor types range from simple pneumatic or electrical switches to Smart transmitters with on-board diagnostics. These sensors are dedicated to SIS service and have process taps which are separate and distinct from the process taps used by normal process information sensors.

Logic Solver: The purpose of this component of SIS is to determine what action is to be taken based on the information gathered. Highly reliable logic solvers are used which provide both fail-safe and fault-tolerant operation. It is typically a controller that reads signals from the sensors and executes preprogrammed actions to prevent a hazard by providing output to final control element(s).

Final Control Element: It implements the action determined by the logic system. This final control element is typically a pneumatically actuated on-off valve operated by solenoid valves.

It is imperative that all three elements of the SIS system function as designed in order to safely isolate the process plant in the event of an emergency.

Safety Standards

In a process plant there is no such thing as risk-free operation or 100% reliability. Therefore, one of the first tasks of the SIS system designer is to perform a risk-tolerance analysis to determine what level of safety is needed. IEC Standard 61508 (Functional Safety of Electric, Electronic and Programmable Electronic Systems) is a general standard that covers functional safety related to all kinds of processing and manufacturing plants. IEC Standard 61511 and ISA S84.01 (Replaced by ISA 84.00.01-2004) are standards specific to the process industries. These standards specify precise levels of safety and quantifiable proof of compliance.

Safety Integrity Level (SIL)

Safety Integrity Levels (SIL) are quantifiable measurement of Risk. Since they were first introduced, Safety Integrity Levels (SIL) have been used as a quantifiable way to establish safety performance targets for SIS systems. IEC standards specify four possible Safety Integrity Levels (SIL1, SIL2, SIL3, SIL4); however, ISA S84.01 only recognizes up to SIL3 levels, as shown in table 1.

Table 1. Safety Integrity Levels: Target Failure Measures

SAFETY INTEGRITY LEVEL (SIL)	REQUIRED SAFETY AVAILABILITY (RSA)	AVERAGE PROBABILITY OF FAILURE ON DEMAND (PFD)
1	90 – 99%	0.1 to 0.01
2	99 – 99.9%	0.01 to 0.001
3	99.9 – 99.99%	0.001 to 0.0001
4	99.99% – 99.999%	0.0001 to 0.00001

A determination of the target Safety Integrity Level requires:

1. An identification of the hazards involved.
2. Assessment of the risk of each of the identified hazards.
3. An assessment of other Independent Protection Layers (IPLs) that may be in place.

Hazards can be identified using a number of different techniques. A risk factor must then be determined for each of the defined hazards. Risk is a function of the probability (likelihood or frequency) and consequences (severity) of each hazardous event.

Table 2 illustrates five different levels of risk that can be identified based on frequency of occurrence.

Table 2. Risk Level Factors Based on Frequency

RISK LEVEL	DESCRIPTIVE WORD	FREQUENCY OF OCCURRENCE
5	Frequent	One per year
4	Probable	One per 10 years
3	Occasional	One per 100 years
2	Remote	One per 1,000 years
1	Improbable	One per 10,000 years

Table 3. illustrates another five levels of risk that can be identified based on severity of the occurrence.

Table 3. Risk Level Factors Based on Severity

RISK LEVEL	DESCRIPTIVE WORD	POTENTIAL CONSEQUENCES TO PERSONNEL
5	Catastrophic	Multiple deaths
4	Severe	Death
3	Serious	Lost time accident
2	Minor	Medical treatment
1	Negligible	No injury

Note: The analyst can also take into account the severity of potential consequences to the environment and/or to financial losses from production or equipment damage.

The total overall risk can be determined by multiplying the Risk Level factors from tables 2 and 3 together to obtain a number from 1 to 25. If this product falls between 15 and 25, the risk is considered high and would indicate a possible need for a SIL3. For a product between 6 and 15, the risk is considered moderate and a SIL2 may be called for. If the product falls between 1 and 6, the risk is considered low and a SIL1 may be adequate.

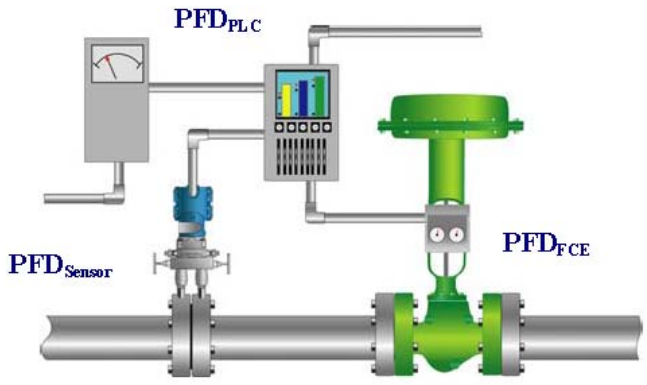
An analysis needs to be performed for each hazardous event for each safety function. Once this is done, the analyst needs to consider the level of protection that may be provided by other Independent Protection Layers (IPLs) such as; basic process control functions, alarms and operator intervention, physical protection such as relief devices or dikes, plant emergency response measures, community emergency measures, etc. Refer to figure 1.

Taking all of these factors into consideration, the analyst then can assign an overall SIL target level to each SIS system. The designer then must design the SIS system equipment to possess probability of failure on demand (PFD) characteristics that will meet that Safety Integrity Level.

Probability of Failure upon Demand (PFD)

By understanding how the components of the SIS system can fail, it is possible to calculate a Probability of Failure on Demand (PFD). There are two basic ways for SIS systems to fail. The first way is commonly called a nuisance or spurious trip which usually results in an unplanned but safe process shutdown. While there is no danger associated with this type of SIS failure, the operational costs can be enormous. The second type of failure does not cause a process shutdown or nuisance trip. Instead, the failure remains undetected, permitting continued process operation in an unsafe and dangerous manner. If an emergency demand occurred, the SIS system would be unable to respond properly. These failures are known as covert or hidden failures and contribute to the probability (PFD) of the system failing in a dangerous manner on demand.

The PFD for the SIS system is the sum of PFDs for each element of the system (see figure 3). In order to determine the PFD of each element, the analyst needs documented, historical failure rate data for each element. This failure rate (dangerous) is used in conjunction with the Test Interval (TI) term to calculate the PFD. It is this test interval (TI) that accounts for the length of time before a covert fault is discovered through testing. Increases in the test interval directly impact the PFD value in a linear manner; i.e., if you double the interval between tests, you will double the Probability for Failure on Demand, and make it twice as difficult to meet the target SIL.



Total Loop SIL =
PFD_{PLC} + PFD_{Sensor} +PFD_{FCE}

Figure 3. PFD of each component of SIS need to include in SIL calculation

The governing standards for Safety Instrumented Systems state that plant operators must determine and document that equipment is designed, maintained, inspected, tested, and operated in a safe manner. Thus, it is imperative that these components of Safety Instrumented System be tested frequently enough to reduce the PFD and meet the target SIL.

DVC6000 SIS Training Course 1

September 2005

Quiz

1. SFF (Safe Failure fraction) is ratio of
   a. Safe Failures / Dangerous Failures
   b. Safe Failures / Total Failures
   c. Dangerous Detected Failures / Total Failures
   d. All Failures except Dangerous Undetected Failures / Total Failures
2. Which one is a true statement?
   a. Standard IEC61508 (Functional Safety of Electric, Electronic and Programmable Electronic Systems) is a general standards that covers functional safety related to equipment manufacturing, and IEC Standard 61511 is specific to the process industries.
   b. Standard IEC61508 (Functional Safety of Electric, Electronic and Programmable Electronic Systems) is a general standards that covers functional safety related to process industries, and IEC Standard 61511 is also to the process industries.
   c. Standard IEC61508 (Functional Safety of Electric, Electronic and Programmable Electronic Systems) is a general standards that covers functional safety related to process industries, and IEC Standard 61511 is guidelines to equipment manufacturers.
   d. None of the above
3. SIL is quantitative measure of Risk and Risk is a function of
   a. Frequency
   b. Consequences
   c. Frequency & Consequences
   d. None of the above
4. SIL 4 is rarely used in process industry:
   a. True
   b. False
   c. Maybe
   d. None of the above
5. If a customer needs to compute PFD_{avg} of Safety Instrumented Function (SIF), he needs
   a. MTBF of each component in the SIF loop
   b. Require Dangerous Failure rates of each components in the loop
   c. Require Safe Failure rates of each components in the loop
   d. Require Dangerous and Safe Failure rates of each components in the loop

Answers Key: 1) d; 2) a; 3) c; 4) a; 5) b

Emerson Process Management

Fisher
Marshalltown, Iowa 50158 USA
Cernay 68700 France
Sao Paulo 05424 Brazil
Singapore 128461

www.Fisher.com